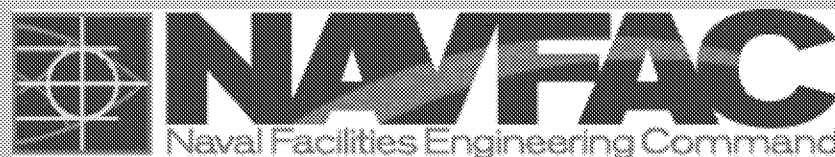**From:** Navy Base Realignment and Closure (BRAC) [info@sfhpns.com]
Sent: 7/19/2017 5:05:18 AM
To: LEE, LILY [LEE.LILY@EPA.GOV]
Subject: Hunters Point Naval Shipyard - Radiological Technical Advisor Available in Bayview Hunters Point - August 5, 6, 7

Ask An Expert

Community Technical Advisor Available to Answer Questions About Radiological Health and Safety at Upcoming Local Outreach Events

Dr. Kathryn Higley, Community Technical Advisor from Oregon State University

Dr. Kathryn Higley will be available to meet with community members individually or in small, informal group settings to answer questions and provide information on radiological health and safety. Drop in to meet her anytime between 10:30 a.m. and noon on one of the following days:
* Saturday, August 5, 2017
* Sunday, August 6, 2017
* Monday, August 7, 2017
Each session will be held at The Storehouse, 451 Galvez Avenue, San Francisco 94124 (map provided below)

*Dr. Higley, who provides support to community members in her role as a **Community Technical Advisor** for the greater Hunters Point community, is an internationally respected expert in radiological health and safety from Oregon State University.*

Contact Information for Dr. Higley

If you are unable to visit with Dr. Higley in person, she is available for questions from the greater Hunters Point community. She may be reached by phone at (541) 737-7063 or by email at Kathryn.Higley@oregonstate.edu.

Map to The Storehouse, 451 Galvez Avenue, San Francisco 94124

Click here to visit the Navy's Radiological Cleanup Page for Hunters Point Naval Shipyard.

Updated Documents Available on Navy Website

Visit the Navy's website for information on the environmental cleanup at HPNS. Recent uploaded documents include the most recent Quarterly Progress Update (2nd Quarter 2017) and the Parcel E-2 Air Monitoring Fact Sheet. Additional historical program documents are available on the web pages, as well as searchable through the online Administrative Record.

Subscribe now for updates and more information!

New Website Security Certificate Information

The American people expect government websites to be secure and their interactions with those websites to be private. **When visiting the Navy's website, expect a security certificate message.**

The White House Office of Management and Budget (OMB) Memorandum M-15-13, "A Policy to Require Secure Connections across Federal Websites and Web Services" requires that all publicly accessible Federal websites and web services only provide service through the use of a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS) which many commercial organizations have implemented to protect visitors to their websites and services.

The Federal government and NAVFAC are adapting to this changing landscape. The NAVFAC Public website implemented Hypertext Transfer Protocol Secure (HTTPS) in January 2017. These Certificates ensure that your computer can recognize and guarantee the integrity of the connection between the NAVFAC Web site and your computer. If you choose NOT to take advantage of installing these certificates, you will receive a certificate warning page indicating "There's a problem with this websites security certificate" each time you connect to this site. Additionally, you should update all bookmarks that you may have saved to specific pages to reflect this change in protocols. **Instructions on how to install the Department of Defense (DoD) Certificates is provided below.**

If you have any questions about this procedure or problems downloading the certificate after following the instructions, please contact

disa.meade.re.mbx.iase-website@mail.mil. If you would like a copy of the PDF document with the instructions (see below) emailed to you, please call the HPNS Info Line at (415) 295-4742 or send an email to info@sfhpns.com.

DoD Root Certificates Installation Procedure

Secure websites (HTTPS) use digital certificates to establish secure connections via Public Key Infrastructure (PKI). In order for a web browser to properly authenticate the identity of a secure website, it must know to communicate with the Certificate Authority (CA) that issues the site its digital certificate. Most web browsers already have commercial CA certificates associated. However, military hosting utilizes its own CA's.

As CNIC is subject to the rules set by Federal, DOD, and DON laws and regulations, you may need to manually install the DoD CA certificates on your personal or non-DoD computer in order to access our public websites via a secure connection. DoD-issued computers and users who have non-DOD computers who access DOD assets generally have these certificates and are up-to-date.

To download the DoD CA certificates:

*Please access: http://iase.disa.mil/pki-pke/Pages/tools.aspx
*Select the heading for "Trust Store."
*Under the heading for "InstallRoot 5.0.1 NIPR Windows Installer," please select the link for "Non Administrator."
*You will be prompted to Open/Run/Save the installation file, "InstallRoot_5.0.1x32_NonAdmin.msi." The need to save is not required, so it is your preference on which of the available options you choose.
*Upon opening the "InstallRoot_5.0.1x32_NonAdmin.msi" file, you will be presented with the InstallRoot Setup Wizard. Simply choose "Next" after reading each step of the Wizard.
*When prompted to select the features you wish to install, ensure that *at least* the "Graphical Interface" is checked. Afterwards, click on "next" and then "install."
*After the installation of the tool is complete, click "Run InstallRoot."
*At this point, you may be prompted to add the certificates to Firefox (if installed on your computer).
*A "Quick Start" screen will appear showing screenshots of the final steps required to complete the installation. Please read the red text within these screenshots and choose "Next" until you're able to select "Finish."
*After selecting "Finish," you should be presented with a Microsoft Current User tab and, if you chose to install certificates to Firefox as indicated in step #8, a Firefox tab should also appear for each Firefox profile on your computer. Please look under each of these tabs and make sure that "Install DoD Certificates" has a green checkmark. The other certificates (ECA and JITC) are not required.
*Click on the "Install Certificates" button.

Web
Vers
ion
Forw
ard
Uns
ubsc
ribe